

Exhibit 5

DECLARATION OF THOMAS KIERNAN

I am over the age of eighteen and not a party to this action. I am providing this Declaration in support of Defendant Roman Storm's Motion in Limine to Exclude and/or Limit Proposed Expert and Lay Witness Testimony in United States v. Storm, Case No. 23 Cr. 430 (KPF). The following is based on my own personal knowledge, education, training, and experience.

I. BACKGROUND AND QUALIFICATIONS

1. I am a Partner and Co-Founder of NAXO Labs, LLC ("NAXO"). NAXO is a blockchain and cyber investigations firm located in New York, New York. In connection with my work at NAXO, I routinely conduct forensic investigations involving computers, mobile devices, and other electronic evidence. I also regularly provide expert consultation to clients, including law enforcement, regulatory agencies, legal counsel, and private corporations and individuals regarding computer and network security best practices, forensic investigations, cyber incident response, and related investigative analysis.

2. I was previously employed by the Federal Bureau of Investigation ("FBI") for approximately twenty-three years, including most recently serving as a Computer Scientist for the FBI's New York Cyber Crime Division from 2001 to 2014. I have participated in hundreds of criminal and national security cyber investigations, where, among other duties, I collected, reviewed, and analyzed digital evidence using a variety of forensic tools. I have been certified as an FBI Computer Analysis Response Team ("CART") Technician/Forensic Examiner for both criminal and national security cases. Those certifications were in the Windows and Linux operating systems, along with mobile devices. I received both the United States Attorney General's Award and the FBI Director's Award for Outstanding Cyber Investigations in connection with my work.

3. From 2014 to 2015, I was employed as a Senior Director in FTI Consulting, Inc.'s ("FTI") Global Risk and Investigations Practice in the Cyber Security & Investigations Group. From 2015 to 2022, I was employed as a Director at Berkeley Research Group, LLC ("BRG") in BRG's Cyber Operations & Incident Response Practice. At both BRG and FTI, my work was substantially similar to the services I currently provide at NAXO.

4. I earned a B.S. in Computer Science from St. John's University in 1991. I have been certified as a Certified Forensic Computer Examiner ("CFCE") by the International Association of Computer Investigative Specialists ("IACIS") and as an AccessData Certified Examiner ("ACE"). I am also certified as a Cellebrite Certified Mobile Examiner ("CCME").

5. I have testified as an expert in connection with several criminal and civil matters regarding computer artifacts identified through forensic examinations that I conducted of computers and mobile devices. I have also submitted expert reports and declarations pertaining to recovering and interpreting artifacts recovered from computer log files and other digital media.

6. I am being compensated for my work on this matter at my standard hourly billing rate of \$600.00. All the opinions and conclusions stated in this declaration are my own. My compensation is not contingent upon my opinions, testimony, or the outcome of this matter.

7. A copy of my Curriculum Vitae is attached to this Declaration as **Exhibit A**.

II. SUMMARY OF ANALYSIS & OPINION

8. I have been retained by legal counsel for the Defendant, Roman Storm, to conduct a forensic analysis of certain electronic files provided with the government's disclosure of the anticipated testimony of Mr. Philip Werlau, to determine, to the extent possible, (a) when those files were created and/or modified, (b) any associated information regarding the authorship of

those documents, and (c) whether that information, if present, indicates that any of the documents were authored or last modified by Mr. Werlau.

9. Counsel for the Defendant provided NAXO with access to a secure file transfer site that contained the files I reviewed in preparing this declaration. The files I reviewed and their MD5 hash values¹ are summarized in **Exhibit B**.

10. In conducting my analysis, I identified, extracted, and reviewed metadata and other information embedded within the files. Metadata, generally, refers to data embedded within an electronic file, either automatically by the software used to create the file or manually by the user of the software, and is often used to provide additional information about the file, such as its author, creation date, and modification history.

11. Not all computer files contain metadata. Certain basic types of computer files, such as “plain” text files and comma-separated values (or “CSV”) files, do not typically contain well-defined metadata. More complex types of computer files, such as Adobe Portable Document Format (“PDF”) files and files created using software like Microsoft Word and Excel, often (but not always) contain metadata providing historical information regarding the creation and modification of the file itself.

12. The files that I reviewed in connection with this declaration are types of files that, in my experience, typically include metadata. I understand that the contents of the files I reviewed relate to analysis performed in connection with Mr. Werlau’s expert disclosures, though the scope of my own analysis described herein is limited to a forensic analysis of metadata and other artifacts within the files rather than their human-readable content.

¹ A “hash” or “hash value” is the output of a mathematical function (called a “hash function”) often used in cryptography to derive a unique “fingerprint” for a computer file or other source of electronic data. “MD5” is a hash function commonly used in the field of computer forensics for verifying the integrity of data.

13. I did not identify any metadata or other forensic artifacts in the files I reviewed that indicated the files were created, authored, or last modified by Mr. Werlau.

III. METHODOLOGY & ANALYSIS OF DOCUMENT METADATA

14. I used an industry-standard computer forensics software tool called Forensic Toolkit 7.4.2.348 (“FTK”)² to extract and analyze metadata contained within the files identified by counsel in Exhibit B. I also used FTK to compute the MD5 hash values for each of the files as summarized in Exhibit B.

15. I observed that each file in Exhibit B contains embedded metadata, including the author, creation date, modified date, last saved time and other relevant information. The presence of such metadata is consistent with my prior experience analyzing similar files in FTK. I then analyzed each file in Exhibit B individually.

16. I determined that the file “Gas Analysis Methodology.pdf” is a Portable Document Format (“PDF”) document. The metadata within the file indicates that the document was created on or about March 12, 2025, at approximately 11:02:33 PM EDT (2025-03-13 03:02:33 UTC³) and identifies the author of the document as “Marshall Yale.” (**Exhibit C.**)

17. I determined that the file “known_ui_txs.xlsx” is a Microsoft Excel document. The metadata within the file indicates that the document was created and last saved on or about March 10, 2025, at approximately 3:58:18 PM EDT (2025-03-10 19:58:18 UTC) and identifies the name of the user who last saved the file as “Marshall Yale.” The metadata does not identify the author of the document. (**Exhibit D.**)

² AccessData Forensic Toolkit (FTK) is a form of digital forensic investigation software that enables efficient data analysis, evidence processing, and case management. As described above, I have been qualified as an AccessData Certified Examiner regarding the use of FTK in forensic investigations. I regularly use FTK in connection with my work and, in my experience, it is often relied on by other experts in the field of computer forensics.

³ Coordinated Universal Time (UTC) is the global time standard used for regulating clocks, timekeeping, and synchronization across various fields, including computing.

18. I determined that the file “Smart Contract Code and Calls.docx” is a Microsoft Word document. The metadata within the file indicates that the document was created on or about October 23, 2024, at approximately 3:26:00 PM EDT (2024-10-23 19:26:00 UTC) and identifies the author of the document as “Marshall Yale.” Additionally, the metadata indicates that the document was last saved on or about October 23, 2024, at approximately 4:47:00 PM EDT (2024-10-23 20:47:00 UTC) by a user identified as “Marshall Yale.” (**Exhibit E.**)

19. I determined that the file “ui_and_cli_information.docx” is also a Microsoft Word document. The metadata within the file indicates that the document was created on or about October 23, 2024, at approximately 6:42:00 PM EDT (2024-10-23 22:42:00 UTC) and identifies the author of the document as “Marshall Yale.” Additionally, the metadata indicates that the document was last saved on or about October 24, 2024, at approximately 5:32:00 PM EDT (2024-10-24 21:32:00 UTC) by a user identified as “Marshall Yale.” (**Exhibit F.**)

20. I determined that the file “proposals_and_proxy_implementations.xlsx” is a Microsoft Excel document. The metadata within the file identifies the author of the document as “Marshall Yale.” Additionally, the metadata indicates that the document was last saved on or about October 29, 2024, at approximately 2:20:18 PM EDT (2024-10-29 18:20:18 UTC) by a user with the name “Marshall Yale.” The metadata does not contain a timestamp indicating when the document was created. (**Exhibit G.**)

21. I determined that the file “Tornado Cash IP Server.docx” is a Microsoft Word document. The metadata within the file indicates that the document was created on or about October 24, 2024, at approximately 9:13:00 PM EDT (2024-10-25 01:13:00 UTC) and identifies the author of the document as “Marshall Yale.” Additionally, the metadata indicates that the document was last saved on or about October 24, 2024, at approximately 10:28:00 PM EDT

(2024-10-25 02:28:00 UTC) by a user identified as “Marshall Yale.” (**Exhibit H.**) I determined that the file “relayer_information.docx” is a Microsoft Word document. The metadata within the file indicates that the document was created on or about October 21, 2024, at approximately 3:00:00 PM EDT (2024-10-21 19:00:00 UTC) and identifies the author of the document as “Marshall Yale.” Additionally, the metadata indicates that the document was last saved on or about October 24, 2024, at approximately 5:28:00 PM EDT (2024-10-24 21:28:00 UTC) by a user identified as “Marshall Yale.” (**Exhibit I.**)

22. I determined that the file “RelayerStats_Dune_Query.xlsx” is a Microsoft Excel document. The metadata within the file indicates that the document was created on or about February 14, 2025, at approximately 1:47:49 PM EST (2025-02-14 18:47:49 UTC) and identifies the author of the document as “Daniels James P.” Additionally, the metadata indicates that the document was last saved on or about February 14, 2025, at approximately 1:47:49 PM EST (2025-02-14 18:47:49 UTC) by a user identified as “Daniels James P.” (**Exhibit J.**)

23. I determined that the file “TC-Relayer-Analysis.xlsx” is a Microsoft Excel document. The metadata within the file indicates that the document was created on or about March 11, 2025, at approximately 3:59:25 PM EDT (2025-03-11 19:59:25 UTC) and identifies the author of the document as “Daniels James P (CI - Contractor).” Additionally, the metadata indicates that the document was last saved on or about March 12, 2025, at approximately 1:57:41 PM EDT (2025-03-12 17:57:41 UTC) by a user identified as “Daniels James P.” (**Exhibit K.**)

24. I determined that the file “IPFS for pinata.pptx” is a Microsoft PowerPoint document. The metadata within the file identifies the author of the document as “Shaun MaGruder.” Additionally, the metadata indicates that the document was last saved on or about October 17, 2024, at approximately 11:20:16 AM EDT (2024-10-17 15:20:16 UTC) by a user

identified as “Marshall Yale.” The metadata does not contain a timestamp indicating when the document was created. (**Exhibit L.**)

25. I determined that the file “tc_ipfs_changes_and_ens_ownership.xlsx” is a Microsoft Excel document. The metadata within the file indicates that the document was created on or about July 12, 2024, at approximately 1:16:57 PM EDT (2024-07-12 17:16:57 UTC) and identifies the author of the document as “Shawn Johnson.” Additionally, the metadata indicates that the document was last saved on or about October 22, 2024, at approximately 12:08:00 PM EDT (2024-10-22 16:08:00 UTC) by a user identified as “Marshall Yale.” (**Exhibit M.**)

26. I determined that the file “dns_report_tc.xlsx” is a Microsoft Excel document. The metadata within the file indicates that the document was created on or about October 22, 2024, at approximately 4:14:47 PM EDT (2024-10-22 20:14:47 UTC) and identifies the author of the document as “Marshall Yale.” (**Exhibit N.**) Metadata within the file also contained references to a Microsoft SharePoint website with the URL “blocktracecom.sharepoint.com” and the identifier “BlockTraceLLC.”⁴⁵ (**Exhibit O.**)

27. In addition to extracting and analyzing the metadata described above using FTK, I validated my analysis by inspecting each file using the “File Properties” feature to view the documents’ metadata on a forensic workstation running the Microsoft Windows 11 Enterprise Version 23H2 operating system. (**Exhibit P.**) In each case, the document metadata displayed via “File Properties” is consistent with my analysis using FTK.

⁴ https://blocktracecom.sharepoint.com/sites/BlockTraceLLC/Shared Documents/Professional Services/Investigations/TC/ui_hosting_info/ (**Exhibit O.**)

⁵ Based on my review of publicly available information, I identified an individual with a public LinkedIn profile named “Marshall Yale” associated with a blockchain forensics company called BlockTrace. (**Exhibit R.**)

28. I also used the program Adobe Acrobat Reader Version 2025.001.20467⁶ to verify the metadata contained in the file “Gas Analysis Methodology.pdf.” (**Exhibit Q.**)

IV. CONCLUSION


29. As mentioned previously, document metadata, such as the date and time when the document was created and the author of the document, is typically created and updated automatically by the software used to create the document (e.g., Microsoft Word or Adobe Acrobat) based on information from the computer on which the document is created or modified. Consequently, document metadata can sometimes be manipulated by changing the name of the user or the time on the computer on which the document is created, which can result in inconsistencies between metadata fields within a document or between documents from the same source. I did not observe any such inconsistencies during my analysis described herein.

30. None of the metadata contained within the documents I analyzed indicated that the documents were authored or edited by Mr. Werlau.

DECLARATION STATEMENT

I declare under the penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Dated: New York, New York
June 6, 2025



Thomas Kiernan

⁶ Adobe Acrobat Reader is a widely used PDF viewer developed by Adobe, providing tools for viewing, annotating, and managing PDF documents.

EXHIBIT A

CV OF THOMAS J. KIERNAN

[Remainder of this page intentionally blank]

CURRICULUM VITAE

Thomas Kiernan

NAXO



Thomas Kiernan

**PARTNER & CO-FOUNDER
NAXO**

45 Rockefeller Plaza, Suite 1964, New York, NY 10111
tkiernan@naxo.com | www.naxo.com

A former computer scientist for the FBI, Tom Kiernan specializes in digital forensic analysis and investigations involving emerging technologies and complex datasets. During his 23-year career with the FBI's New York field office, Tom provided technical and forensic investigative support to criminal, terrorism, and national security cases. He is a recipient of the US Attorney General's Award for Outstanding Cyber Investigation and the FBI Director's Award for Outstanding Cyber Investigations.

In his role at the FBI, Tom served for over 23 years specializing in incident response and computer forensic investigations. His experience spans high-profile investigations including the notorious billion-dollar underground cryptocurrency-based Silk Road and Silk Road 2.0 drug marketplaces; the Anonymous/LulzSec hacktivist groups; Operation Dirty R.A.T. targeting the creators and users of Black Shades spyware; the hacks of Citibank, PNC Bank, and JP Morgan Chase Bank; Operation Card Shop, which targeted identity thieves in the largest ever online undercover operation; and the takedown of a multi-million computer botnet in Operation Ghost Click.

Since leaving government service, Tom has leveraged his specialized skills to help businesses and government agencies collect and analyze data from a wide variety of sources, including computer and mobile devices and emerging technologies such as cloud-based platforms, encrypted devices, and cryptocurrency wallets. Tom has worked with clients across diverse industries, including healthcare, technology, social media, government, finance, retail, and education.

Tom holds a BS in Computer Science from St. John's University. He is a Cellebrite Certified Mobile Examiner (CCME) and has held a Certified Forensic Computer Examiner (CFCE) certification from the International Association of Computer Investigative Specialists (IACIS). He is also a member of the Information Systems Audit and Control Association (ISACA). Tom has been qualified as an expert witness in computer forensics in numerous cases in federal court.

EDUCATION

B.S., COMPUTER SCIENCE
St. John University, 1991

CERTIFICATIONS

Access Data FTK Certified Examiner
Cellebrite Certified Mobile Examiner
Cellebrite Certified Physical Analyst
Certified Forensic Computer Examiner
Cellebrite Certified Logical Analyst
FBI Computer Analysis Response Team –
Forensic Technician

PRIOR EXPERIENCE

BERKELEY RESEARCH GROUP

New York, NY

Director, Cyber Operations & Incident Response
2015 – 2022

- Built out advanced mobile forensics team capable of complex recovery and analysis of data stored on cellular devices.
- Supervised the forensic imaging and investigation of over 500 mobile devices for a federal government agency. Supervised a team of four investigators utilizing Cellebrite's software suite to preserve and analyze device data in support of active criminal investigations.
- Conducted forensic evidence collection and analysis in response to breaches of client networks by external threats and theft of proprietary information by corporate insiders.
- Executed penetration testing and vulnerability assessments of client networks.
- Retained as an expert in a variety of civil and criminal matters related to computer forensics and cybersecurity.

FTI CONSULTING

New York, NY

Senior Director, Cyber Security & Investigations
2014 – 2015

- Led or supported computer and network forensic investigations and vulnerability assessments as a member of FTI's Cyber Security & Investigations Group
- Collected and forensically analyzed computer data to support ongoing litigation and investigations using methods consistent with those used by the FBI.
- Built and maintained forensics laboratory capable of supporting a broad range of digital investigations.

FEDERAL BUREAU OF INVESTIGATION

New York, NY

Computer Scientist
2001 – 2014

- Served as the technical expert supporting the FBI's most critical criminal and national security cases during his tenure, including Silk Road, Operation R.A.T., Carder Profit investigation and the takedown of Anonymous/LulzSec.
- Responsible for forensic processing and analysis of data related to cases run out of the FBI's New York office, which is the FBI's largest office.
- Recovered deleted or locked data that led to numerous criminal convictions and ensured the safety of the nation's infrastructure.
- Developed forensic methods and standards that are still used by the FBI today; trained numerous FBI agents and civilian employees on forensic best practices.
- Testified to forensic methods in Federal court on multiple occasions.
- Recipient of the US Attorney General's Award for Outstanding Cyber Investigation and the FBI Director's Award for Outstanding Cyber Investigations.

EXPERT TESTIMONY

- *Devin A. Marino v. Timothy I. Duffy*, Superior Court of New Jersey, Case No. FV-10-000189-24. Designated by the Court as a testifying expert in computer and mobile device forensics. Provided expert testimony at trial.
- *Williams and Wilbert v. First Student*, United States District Court for the District of New Jersey, Case No. 20-cv-001176. Designated by the Defendant as testifying computer forensics expert; provided deposition testimony.
- *Paul Iacovacci v. Brevet Holdings, LLC*, United States District Court for the Southern District of New York, Case No. 18- cv- 08048. Designated by the Plaintiff as testifying computer forensics expert; provided deposition testimony.
- *United States v. Raheem Brennerman a/k/a "Jefferson R. Brennerman," a/k/a "Ayodeji Soetan"*. United States District Court for the Southern District of New York. Case No. 17-cr-337. Designated by Plaintiff as testifying computer forensics expert; provided trial testimony.
- *Securities and Exchange Commission v. Chad C. McGinnis, et al.*; United States District Court of Vermont; Civil Action No. 5:14-CV-6. Expert declaration and expert report. The analysis identified two fabrications in Plaintiff's expert testimony.
- *Azima v. RAK Investment Authority*, United States District Court for the District of Columbia; Case No. 16- CV- 01948- KBJ. Served as an expert on behalf of the Defendant on the anonymity provided by the use of a BitTorrent sites and the fact that internet search engines do not provide an index of the content of BitTorrent sites users.

FACT WITNESS TESTIMONY

- *United States v. The Blacksands Pacific Group, Inc & Raheem Brennerman*. United States District Court for the Southern District of New York. Case No. 17-cr-0155 (LAK). Provided fact witness testimony at trial regarding computer forensics and digital artifact retrieval.
- *United States v. Greg Jones*, United States District Court for the Southern District of New York, Case No.18- cr- 662 (JGK) (U.S. District Court for the Southern District of New York). Provided fact witness testimony at trial regarding digital evidence retrieved from a cell phone.
- *United States v. Ross William Ulbricht, a/k/a "Dred Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road"*. United States District Court for the Southern District of New York, Case No. 14-cr-68 (KBF). Provided fact witness testimony at trial regarding computer forensics techniques and digital artifact retrieval.

PROFESSIONAL TRAINING

- Nov 2022 – Cellebrite Certified Mobile Examiner Re-Cert (CCME)
- Sept 2020 – ACE Certification Access Data
- Nov 2018 – SANS 500 Windows Forensics Analysis
- Nov 2018 – Cellebrite Certified Mobile Examiner Re-Cert (CCME)
- Dec 2016 – Cellebrite Certified Mobile Examiner (CCME)
- Nov 2016 – Cellebrite Certified Physical Analyst (CCPA)
- Nov 2016 – Cellebrite Certified Logical Analyst (CCLO)
- Jan 2015 – Cellebrite Mobile Forensic Fundamentals (CMFF)
- Sept 2014 – FBI - AccessData – Case Agent Investigation Review (CAIR) Training

PROFESSIONAL TRAINING (CONT'D)

- May 2013 – FBI – Cyber Division Training – Cyber 1500 Linux for LEO
- Feb 2013 – FBI – CART Imaging Competency Certification Training Recertification
- May 2009 – FBI – CART Imaging Competency Certification Training
- Nov 2008 – FBI – Cyber Investigative Techniques and Resources Computer Based Training
- Mar 2008 – SANS Network Penetration Testing and Ethical Hacking
- Sept 2007 – SANS Network Security - Hacker Techniques and Incident Handling
- Mar 2007 – SANS Security Essentials - Bootcamp Style
- Jan 2007 – National White Collar Crime Center – Internet Investigations - Computer Based Training
- May 2005 – FBI Wintel Certification Training – Write Protect and Imaging - FBI Forensic Laboratory
- Jan 2004 – FBI – Cyber Division – Solaris Log Analysis and Investigation
- Dec 2003 – FBI – Cyber Division – Solaris Advanced System Administration
- Sept 2002 – Red Hat Inc. RH133 - Red Hat Linux System Administration
- Sept 2002 – Red Hat Inc. RH033 – Red Hat Linux Essentials
- May 2002 – Computer Security Institute – Windows NT – Information Security Seminars
- Dec 2001 – FBI – Cyber Division – Solaris System Administration

REPRESENTATIVE MATTERS**DIGITAL FORENSICS INVESTIGATIONS**

- Provide ongoing support to a US federal law enforcement agency in connection with darknet investigations and digital forensics. Services include training and technical assistance related to investigative tools used to collect and analyze data.
- Retained by the U.S. Attorney's Office, Southern District of New York to forensically process and analyze over 500 iPhone, Android, and Nextel phones, various personal computers, PCIe-based drives, servers, and other devices belonging to drug overdose victims. Used standard forensic tooling, including Tableau, Cellebrite, and FTK, as well as proprietary techniques to recover and extract relevant data, including emails, messages, and geolocation data from devices and transmit evidence to law enforcement personnel. Evidence identified led to multiple arrests and convictions.
- Retained by the U.S. Attorney's Office, Southern District of New York to forensically process and analyze hard drives and mobile devices belonging to an individual accused of running a tens-of-millions dollar fraud scheme related to a fictitious company. Compiled evidence and provided testimony at trial, which resulted in a conviction.
- Retained by counsel on behalf of a major transportation company engaged in litigation related to a school bus accident. Conducted forensic analysis of a digital video recording (DVR) device in connection with allegations that the client spoliated evidence by deleting video footage. Determined that footage was not actually deleted and provided an expert report and deposition demonstrating conclusions.
- Retained by counsel as a technical expert on behalf of an individual accused of making a false statement to the FBI. Conducted a review of domain name system (DNS) log files and other relevant evidence and provided client with a verbal assessment of findings as well as a technical explanation of how DNS works.
- Retained by counsel on behalf of an individual who accused his former employer of illegally accessing his computer and obtaining his personal data. Conducted a forensic analysis that identified unauthorized logins to the client's account on the device; provided an expert report and deposition that detailed the findings.

DIGITAL FORENSICS INVESTIGATIONS (CONT'D)

- Retained as a computer forensics expert by a U.S. regulatory agency to assist in executing a search warrant as well as to provide forensic analysis of seized devices. Services included collecting, analyzing, and preserving hard drives and mobile devices and preparing evidence for a possible Federal trial.
- Retained through counsel by an individual who was accused of insider trading by the U.S. Securities and Exchange Commission. Provided forensic analysis, expert opinions, and sworn testimony that identified flaws in key evidence presented by prosecution. The trial resulted in a victory for the defendant.
- Retained by counsel to forensically collect and preserve highly sensitive tax information from a propriety software platform used by an accounting firm in connection with a Congressional investigation.

CYBER SECURITY

- Retained by a Colorado-based car dealership to conduct technical penetration testing and vulnerability assessments of its IT infrastructure, which included wireless access points installed throughout the company's campus. Identified numerous vulnerabilities and a provided prioritized list of recommended remediations.
- Provided on-site incident response for a billion-dollar travel company that fell victim to a cyber attack. Provided digital forensics in support of a successful root cause investigation as well as ongoing consulting services related to internal cybersecurity initiatives.
- Engaged by a law firm to investigate and mitigate an email breach against the firm's client. The investigation revealed that the attacker had access to several employees' accounts at the company and fraudulently moved funds from the firm.
- Retained by a New York-based consulting firm to conduct an independent network security assessment and penetration test. Provided a report that included prioritized recommendations and assisted in implementing fixes of critical vulnerabilities.

EXHIBIT B**DOCUMENTS ANALYZED**

File Name	MD5 Hash
Gas Analysis Methodology.pdf	4d199b1bfb6ce861e815a306c90effb2
known_ui_txs.xlsx	a00f804f40f3a2c1ccb04e9c4cea8e08
Smart Contract Code and Calls.docx	b033675fce862fc21e8454b52331c315
ui_and_cli_information.docx	bbdbf03689558623f106894614b45dc0
dns_report_tc.xlsx	5e8c9af81a62e29c7faa1eae99dcbb9
proposals_and_proxy_implementations.xlsx	327cb5a93666c7286d888c9db420df8e
Tornado Cash IP Server.docx	6e5ac5f3a2af995bfbdbab1b94e5b92a
relay_information.docx	63852d8380647f0bf8756f84e45fab4c
RelayerStats_Dune_Query.xlsx	eb4ec936ae8c51f7823ba827a88151f5
TC-Relayer-Analysis.xlsx	9b9c8c80cfbf62c3443f658e3075b58d
IPFS for pinata.pptx	03a6f6b3d9f8de3ee207fa66cb21ab5b
tc_ipfs_changes_and_ens_ownership.xlsx	5409cffc6aa8704ef6ed0b142fc4fecc

EXHIBIT C**FTK DOCUMENT METADATA ANALYSIS**

Name	Gas Analysis Methodology.pdf
Item Number	1251
File Type	Adobe Acrobat
Path	Government Disclosures [AD1]/Rebuttal Disclosure Materials.zip»
[-] General Info	
[-] File Size	
[-] File Dates	
[-] File Attributes	
[-] General	
Actual File	False
Compressed Size	524,364
Compressed	True
File Type (FBFS)	PDF
FBFS has been examined/enumerated	True
File has been examined for slack	True
Child Order	0
Date Created (metadata)	3/12/2025 11:02:33 PM (2025-03-13 03:02:33 UTC)
Date Modified (metadata)	3/12/2025 11:02:37 PM (2025-03-13 03:02:37 UTC)
[-] Zip Properties	
Checksum	6A39B2B0
Extract Version	2.0
Compression Method	Deflated
[-] Microsoft Office Metadata	
Author	Marshall Yale
[-] PDF Properties	
Creator	Acrobat PDFMaker 24 for Word
Producer	Adobe PDF Library 24.5.168
[-] File Content Info	
[-] Hash Information	
MD5 Hash	4d199b1bfb6ce861e815a306c90effb2
SHA-1 Hash	e1cf3d2b31cea31539f8a33d993d96a2ba2831ba
SHA-256 Hash	

“Gas Analysis Methodology.pdf”

EXHIBIT D**FTK DOCUMENT METADATA ANALYSIS**

Name	known_ui_txs.xlsx
Item Number	1255
File Type	Excel 2016
Path	Government Disclosures [AD1]/Rebuttal Disclosure Materials.zip»known_ui_txs.xlsx
General Info	
File Size	
File Dates	
File Attributes	
General	
Actual File	False
Compressed Size	9,340
Compressed	True
File Type (FBFS)	Zip
File has been examined for slack	True
Child Order	4
Zip Properties	
Checksum	F2E987D2
Extract Version	2.0
Compression Method	Deflated
File System Information	
UTC Timestamps	False
Microsoft Office Metadata	
Last saved by	Marshall Yale
Create time	3/10/2025 3:58:18 PM (2025-03-10 19:58:18 UTC)
Last saved time	3/10/2025 3:58:18 PM (2025-03-10 19:58:18 UTC)
Creating application	Microsoft Excel
Security	0
Crop or Scale	False
Document Sections Count	Worksheets= 1
Document Section Titles	known_ui_txs
Up-to-date Links	False
Track Changes	False
Hidden Worksheets	False
Hidden Columns/Rows	False
File Content Info	
Hash Information	
MD5 Hash	a00f804f40f3a2c1ccb04e9c4cea8e08
SHA-1 Hash	028c0690bd20007825e27118a5ecabbeab0c7845

“known_ui_txs.xlsx”

EXHIBIT E**FTK DOCUMENT METADATA ANALYSIS**

Name	Smart Contract Code and Calls.docx
Item Number	1127
File Type	Microsoft Word 2016 XML
Path	Government Disclosures [AD1]/2025.02.18 Expert Disclosure Production.zip»2
<input type="checkbox"/> General Info	
<input type="checkbox"/> File Size	
<input type="checkbox"/> File Dates	
<input type="checkbox"/> File Attributes	
<input type="checkbox"/> General	
Actual File	False
Compressed Size	776,167
Compressed	True
File Type (FBFS)	Zip
File has been examined for slack	True
Child Order	0
<input type="checkbox"/> Zip Properties	
<input type="checkbox"/> File System Information	
UTC Timestamps	False
<input type="checkbox"/> Microsoft Office Metadata	
Author	Marshall Yale
Template	Normal
Last saved by	Marshall Yale
Revision number	10
Total editing time	1 minutes 21 seconds
Create time	10/23/2024 3:26:00 PM (2024-10-23 19:26:00 UTC)
Last saved time	10/23/2024 4:47:00 PM (2024-10-23 20:47:00 UTC)
Number of pages	7
Number of words	1,206
Number of characters	6,637
Creating application	Microsoft Office Word
Security	0
Line Count	55
Paragraphs	15
Crop or Scale	False
Document Sections Count	Title= 1
Up-to-date Links	False
Track Changes	False
<input type="checkbox"/> File Content Info	
<input type="checkbox"/> Hash Information	
MD5 Hash	b033675fce862fc21e8454b52331c315
SHA-1 Hash	262b202004737fc3801db28cc52a0babd4d7ff2a

“Smart Contract Code and Calls.docx”

EXHIBIT F**FTK DOCUMENT METADATA ANALYSIS**

Name	ui_and_cli_information.docx
Item Number	1135
File Type	Microsoft Word 2016 XML
Path	Government Disclosures [AD1]/2025.02.18 Expert Disclosure Production.zip»2
<input type="checkbox"/> General Info	
<input type="checkbox"/> File Size	
<input type="checkbox"/> File Dates	
<input type="checkbox"/> File Attributes	
<input type="checkbox"/> General	
Actual File	False
Compressed Size	1,479,730
Compressed	True
File Type (FBFS)	Zip
File has been examined for slack	True
Child Order	6
<input type="checkbox"/> Zip Properties	
<input type="checkbox"/> File System Information	
UTC Timestamps	False
<input type="checkbox"/> Microsoft Office Metadata	
Author	Marshall Yale
Template	Normal
Last saved by	Marshall Yale
Revision number	125
Total editing time	8 minutes 10 seconds
Create time	10/23/2024 6:42:00 PM (2024-10-23 22:42:00 UTC)
Last saved time	10/24/2024 5:32:00 PM (2024-10-24 21:32:00 UTC)
Number of pages	8
Number of words	1,437
Number of characters	7,908
Creating application	Microsoft Office Word
Security	0
Line Count	65
Paragraphs	18
Crop or Scale	False
Up-to-date Links	False
Track Changes	False
<input type="checkbox"/> File Content Info	
<input type="checkbox"/> Hash Information	
MD5 Hash	bbdbf03689558623f106894614b45dc0
SHA-1 Hash	4a06afb9f4cd48a6762192d2b39093f95cb0371f

“ui_and_cli_information.docx”

EXHIBIT G**FTK DOCUMENT METADATA ANALYSIS**

Name	proposals_and_proxy_implementations.xlsx
Item Number	1106
File Type	Excel 2016
Path	Government Disclosures [AD1]/2025.02.18 Expert Disclosure Production.zip»2025.02.18 Expert Disclosure
General Info	
File Size	
File Dates	
File Attributes	
General	
Actual File	False
Compressed Size	17,214
Compressed	True
File Type (FBFS)	Zip
File has been examined for slack	True
Child Order	0
Zip Properties	
File System Information	
UTC Timestamps	False
Microsoft Office Metadata	
Author	Marshall Yale
Last saved by	Marshall Yale
Last saved time	10/29/2024 2:20:18 PM (2024-10-29 18:20:18 UTC)
Creating application	Microsoft Excel
Security	0
Crop or Scale	False
Document Sections Count	Worksheets=2
Document Section Titles	proposals, proxy_implementations
Up-to-date Links	False
Track Changes	False
Hidden Worksheets	False
Hidden Columns/Rows	False
File Content Info	
Hash Information	
MD5 Hash	327cb5a93666c7286d888c9db420df8e
SHA-1 Hash	bacf8ed15af2c3067a438799875e7e1a509dda37
SHA-256 Hash	

“proposals_and_proxy_implementations.xlsx”

EXHIBIT H**FTK DOCUMENT METADATA ANALYSIS**

Name	Tornado Cash IP Server.docx
Item Number	1110
File Type	Microsoft Word 2016 XML
Path	Government Disclosures [AD1]/2025.02.18 Expert Disclosure Production.zip»2025.02.18 Expert
<input type="checkbox"/> General Info	
<input type="checkbox"/> File Size	
<input type="checkbox"/> File Dates	
<input type="checkbox"/> File Attributes	
<input type="checkbox"/> General	
<input type="checkbox"/> Zip Properties	
<input type="checkbox"/> File System Information	
UTC Timestamps	False
<input type="checkbox"/> Microsoft Office Metadata	
Author	Marshall Yale
Template	Normal
Last saved by	Marshall Yale
Revision number	1
Total editing time	1 minutes 15 seconds
Create time	10/24/2024 9:13:00 PM (2024-10-25 01:13:00 UTC)
Last saved time	10/24/2024 10:28:00 PM (2024-10-25 02:28:00 UTC)
Number of pages	2
Number of words	226
Number of characters	1,245
Creating application	Microsoft Office Word
Security	0
Line Count	10
Paragraphs	2
Crop or Scale	False
Document Sections Count	Title= 1
Up-to-date Links	False
Track Changes	False
<input type="checkbox"/> File Content Info	
<input type="checkbox"/> Hash Information	
MD5 Hash	6e5ac5f3a2af995bffbdbab1b94e5b92a
SHA-1 Hash	1ae2443b0b76ca76d33bc48e125c96eec61ab70b
SHA-256 Hash	

“Tornado Cash IP Server.docx”

EXHIBIT I**FTK DOCUMENT METADATA ANALYSIS**

Name	relayer_information.docx
Item Number	1125
File Type	Microsoft Word 2016 XML
Path	Government Disclosures [AD1]/2025.02.18 Expert Disclosure Production.zip»2025.02.18 E
<input type="checkbox"/> General Info	
<input type="checkbox"/> File Size	
<input type="checkbox"/> File Dates	
<input type="checkbox"/> File Attributes	
<input type="checkbox"/> General	
<input type="checkbox"/> Zip Properties	
<input type="checkbox"/> File System Information	
<input type="checkbox"/> Microsoft Office Metadata	
Author	Marshall Yale
Template	Normal
Last saved by	Marshall Yale
Revision number	69
Total editing time	48 minutes 2 seconds
Create time	10/21/2024 3:00:00 PM (2024-10-21 19:00:00 UTC)
Last saved time	10/24/2024 5:28:00 PM (2024-10-24 21:28:00 UTC)
Number of pages	4
Number of words	708
Number of characters	3,895
Creating application	Microsoft Office Word
Security	0
Line Count	32
Paragraphs	9
Crop or Scale	False
Document Sections Count	Title= 1
Up-to-date Links	False
Track Changes	False
<input type="checkbox"/> File Content Info	
<input type="checkbox"/> Hash Information	
MD5 Hash	63852d8380647f0bf8756f84e45fab4c
SHA-1 Hash	89703d689d9f88f3ef0ae54c42100f3d7e3bc149
SHA-256 Hash	

“relayer_information.docx”

EXHIBIT J**FTK DOCUMENT METADATA ANALYSIS**

Name	RelayerStats_Dune_Query.xlsx
Item Number	1124
File Type	Excel 2016
Path	Government Disclosures [AD1]/2025.02.18 Expert Disclosure Production.zip»2025.02.18 Expert Disclosure
<input type="checkbox"/> General Info	
<input type="checkbox"/> File Size	
<input type="checkbox"/> File Dates	
<input type="checkbox"/> File Attributes	
<input type="checkbox"/> General	
Actual File	False
Compressed Size	10,002
Compressed	True
File Type (FBFS)	Zip
File has been examined for slack	True
Child Order	1
<input type="checkbox"/> Zip Properties	
<input type="checkbox"/> File System Information	
UTC Timestamps	False
<input type="checkbox"/> Microsoft Office Metadata	
Author	Daniels James P
Last saved by	Daniels James P
Create time	2/14/2025 1:47:49 PM (2025-02-14 18:47:49 UTC)
Last saved time	2/14/2025 1:47:49 PM (2025-02-14 18:47:49 UTC)
Creating application	Microsoft Excel
Security	0
Crop or Scale	False
Document Sections Count	Worksheets=1
Document Section Titles	01JM2WFK1XV1YFJTJKPQD7CV6F
Up-to-date Links	False
Track Changes	False
Hidden Worksheets	False
Hidden Columns/Rows	False
<input type="checkbox"/> File Content Info	
<input type="checkbox"/> Hash Information	
MD5 Hash	eb4ec936ae8c51f7823ba827a88151f5
SHA-1 Hash	860e47362e7087d72a995d3c1b755a69aa5d5c4d
SHA-256 Hash	

“RelayerStats_Dune_Query.xlsx”

EXHIBIT K**FTK DOCUMENT METADATA ANALYSIS**

Name	TC-Relayer-Analysis.xlsx
Item Number	1252
File Type	Excel 2016
Path	Government Disclosures [AD1]/Rebuttal Disclosure Materials.zip»TC-Relayer-Analysis.xlsx
<input type="checkbox"/> General Info	
<input type="checkbox"/> File Size	
<input type="checkbox"/> File Dates	
<input type="checkbox"/> File Attributes	
<input type="checkbox"/> General	
Actual File	False
Compressed Size	1,987,975
Compressed	True
File Type (FBFS)	Zip
File has been examined for slack	True
Child Order	1
<input type="checkbox"/> Zip Properties	
<input type="checkbox"/> File System Information	
UTC Timestamps	False
<input type="checkbox"/> Microsoft Office Metadata	
Author	Daniels James P (CI - Contractor)
Last saved by	Daniels James P
Create time	3/11/2025 3:59:25 PM (2025-03-11 19:59:25 UTC)
Last saved time	3/12/2025 1:57:41 PM (2025-03-12 17:57:41 UTC)
Creating application	Microsoft Excel
Security	0
Crop or Scale	False
Document Sections Count	Worksheets=3
Document Section Titles	summary, relayer_classification_totals, tc_withdrawals_relayer_type
Up-to-date Links	False
Track Changes	False
Hidden Worksheets	False
Hidden Columns/Rows	True
<input type="checkbox"/> File Content Info	
<input type="checkbox"/> Hash Information	
MD5 Hash	9b9c8c80cfbf62c3443f658e3075b58d
SHA-1 Hash	58f5ba02747912664b606c0aba06e9b822058a86
SHA-256 Hash	

“TC-Relayer-Analysis.xlsx”

EXHIBIT L**FTK DOCUMENT METADATA ANALYSIS**

Name	IPFS for pinata.pptx
Item Number	1141
File Type	PowerPoint 2016
Path	Government Disclosures [AD1]/2025.02.18 Expert Disclosure Production.zip»2025.02.18 Expert Disclosure P
<input type="checkbox"/> General Info	
<input type="checkbox"/> File Size	
<input type="checkbox"/> File Dates	
<input type="checkbox"/> File Attributes	
<input type="checkbox"/> General	
<input type="checkbox"/> Zip Properties	
<input type="checkbox"/> File System Information	
UTC Timestamps	False
<input type="checkbox"/> Microsoft Office Metadata	
Title	PowerPoint Presentation
Author	Shaun MaGruder
Last saved by	Marshall Yale
Revision number	38
Total editing time	3 hours 2 minutes 38 seconds
Last saved time	10/17/2024 11:20:16 AM (2024-10-17 15:20:16 UTC)
Number of words	26
Creating application	Microsoft Office PowerPoint
Presentation Target	On-screen Show (16:9)
Paragraphs	6
Slides	2
Notes	1
Hidden Slides	0
Multimedia Clips	0
Crop or Scale	False
Document Sections Count	Fonts Used=2, Theme=1, Slide Titles=2
Document Section Titles	Arial, Courier New, BlockTrace, PowerPoint Presentation, ENS Linkup
Up-to-date Links	False
Embedded Comments	False
<input type="checkbox"/> File Content Info	
<input type="checkbox"/> Hash Information	
MD5 Hash	03a6f6b3d9f8de3ee207fa66cb21ab5b
SHA-1 Hash	4319122f5ba2233d8ded3e2a2955e37188ba0a6b
SHA-256 Hash	

“IPFS for pinata.pptx”

EXHIBIT M**FTK DOCUMENT METADATA ANALYSIS**

Name	tc_ipfs_changes_and_ens_ownership.xlsx
Item Number	1145
File Type	Excel 2016
Path	Government Disclosures [AD1]/2025.02.18 Expert Disclosure Production.zip»2025.02.18 Expert Disclosure Production»
<input checked="" type="checkbox"/> General Info	
<input checked="" type="checkbox"/> File Attributes	
<input checked="" type="checkbox"/> General	
Actual File	False
Compressed Size	101,110
Compressed	True
File Type (FBFS)	Zip
File has been examined for slack	True
Child Order	10
<input checked="" type="checkbox"/> Zip Properties	
<input checked="" type="checkbox"/> File System Information	
UTC Timestamps	False
<input checked="" type="checkbox"/> Microsoft Office Metadata	
Author	Shawn Johnson
Last saved by	Marshall Yale
Revision number	0
Create time	7/12/2024 1:16:57 PM (2024-07-12 17:16:57 UTC)
Last saved time	10/22/2024 12:08:00 PM (2024-10-22 16:08:00 UTC)
Creating application	Microsoft Excel
Security	0
Crop or Scale	False
Document Sections Count	Worksheets=8
Document Section Titles	tornadocash.eth ipfs deployment, all_changes, registrant_changes, tc_eth_controller_changes, auth_changes, ENS su
Up-to-date Links	False
Track Changes	False
Hidden Worksheets	False
Hidden Columns/Rows	True
<input checked="" type="checkbox"/> File Content Info	
<input checked="" type="checkbox"/> Hash Information	
MD5 Hash	5409cffc6aa8704ef6ed0b142fc4fecc
SHA-1 Hash	2f51ffb2453fede1a948dd8a62c0c8ea00bb7908
SHA-256 Hash	

“tc_ipfs_changes_and_ens_ownership.xlsx”

EXHIBIT N**FTK DOCUMENT METADATA ANALYSIS**

Name	dns_report_tc.xlsx
Item Number	1143
File Type	Excel 2016
Path	Government Disclosures [AD1]/2025.02.18 Expert Disclosure Production.zip»2
<input type="checkbox"/> General Info	
<input type="checkbox"/> File Size	
<input type="checkbox"/> File Dates	
<input type="checkbox"/> File Attributes	
<input type="checkbox"/> General	
Actual File	False
Compressed Size	79,925
Compressed	True
File Type (FBFS)	Zip
File has been examined for slack	True
Child Order	8
<input type="checkbox"/> Zip Properties	
<input type="checkbox"/> File System Information	
UTC Timestamps	False
<input type="checkbox"/> Microsoft Office Metadata	
Author	Marshall Yale
Last saved by	Marshall Yale
Create time	10/22/2024 4:14:47 PM (2024-10-22 20:14:47 UTC)
Last saved time	10/22/2024 6:37:03 PM (2024-10-22 22:37:03 UTC)
Creating application	Microsoft Excel
Security	0
Crop or Scale	False
Document Sections Count	Worksheets=1
Document Section Titles	dns_report_tc
Up-to-date Links	False
Track Changes	False
Hidden Worksheets	False
Hidden Columns/Rows	True
<input type="checkbox"/> File Content Info	
<input type="checkbox"/> Hash Information	
MD5 Hash	5e8c9af81a62e29c7faa1eaf9dccbb9
SHA-1 Hash	0b33dda53c2892db4a357bd469d5824a5383599c

“dns_report_tc.xlsx”

EXHIBIT O**FTK DOCUMENT METADATA ANALYSIS**

```

▼<workbook xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main"
xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:mc="http://schemas.openxmlformats.org/markup-
compatibility/2006" xmlns:x15="http://schemas.microsoft.com/office/spreadsheetml/2010/11/main"
xmlns:xr="http://schemas.microsoft.com/office/spreadsheetml/2014/revision"
xmlns:xr6="http://schemas.microsoft.com/office/spreadsheetml/2016/revision6"
xmlns:xr10="http://schemas.microsoft.com/office/spreadsheetml/2016/revision10"
xmlns:xr2="http://schemas.microsoft.com/office/spreadsheetml/2015/revision2" mc:Ignorable="x15 xr xr6 xr10 xr2">
  <fileVersion appName="xl" lastEdited="7" lowestEdited="7" rupBuild="28025"/>
  <workbookPr defaultThemeVersion="202300"/>
  ▼<mc:AlternateContent xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006">
    ▼<mc:Choice Requires="x15">
      <x15ac:absPath xmlns:x15ac="http://schemas.microsoft.com/office/spreadsheetml/2010/11/ac"
        url="https://blocktracecom.sharepoint.com/sites/BlockTraceLLC/Shared Documents/Professional
        Services/Investigations/TC/ui_hosting_info"/>
    </mc:Choice>
  </mc:AlternateContent>
  <xr:revisionPtr revIDLastSave="2" documentId="8_{F8979EFE-9FE6-4638-8A47-14B07D6AEA42}" xr6:coauthVersionLast="47"
  xr6:coauthVersionMax="47" xr10:uidLastSave="{44DB98C9-177E-453E-844F-55661DC11B32}"/>
  ▼<bookViews>
    <workbookView xWindow="-96" yWindow="-96" windowWidth="20928" windowHeight="12432" xr2:uid="{959A962F-5842-4DB2-9033-316E116D24CD}"/>
  </bookViews>
  ▼<sheets>
    <sheet name="dns_report_tc" sheetId="1" r:id="rId1"/>
  </sheets>
  ▼<definedNames>
    <definedName name="_xlnm._FilterDatabase" localSheetId="0" hidden="1">dns_report_tc!$A$1:$L$1387</definedName>
  </definedNames>
  <calcPr calcId="191029"/>
  ▼<extLst>
    ▼<ext xmlns:xcalcf="http://schemas.microsoft.com/office/spreadsheetml/2018/calcf" uri="{B58B0392-4F1F-4190-8B64-5DF3571DCE5F}">
      ▼<xcalcf:calcFeatures>
        <xcalcf:feature name="microsoft.com:RD"/>
        <xcalcf:feature name="microsoft.com:Single"/>
        <xcalcf:feature name="microsoft.com:FV"/>
      </xcalcf:calcFeatures>
    </ext>
  </extLst>

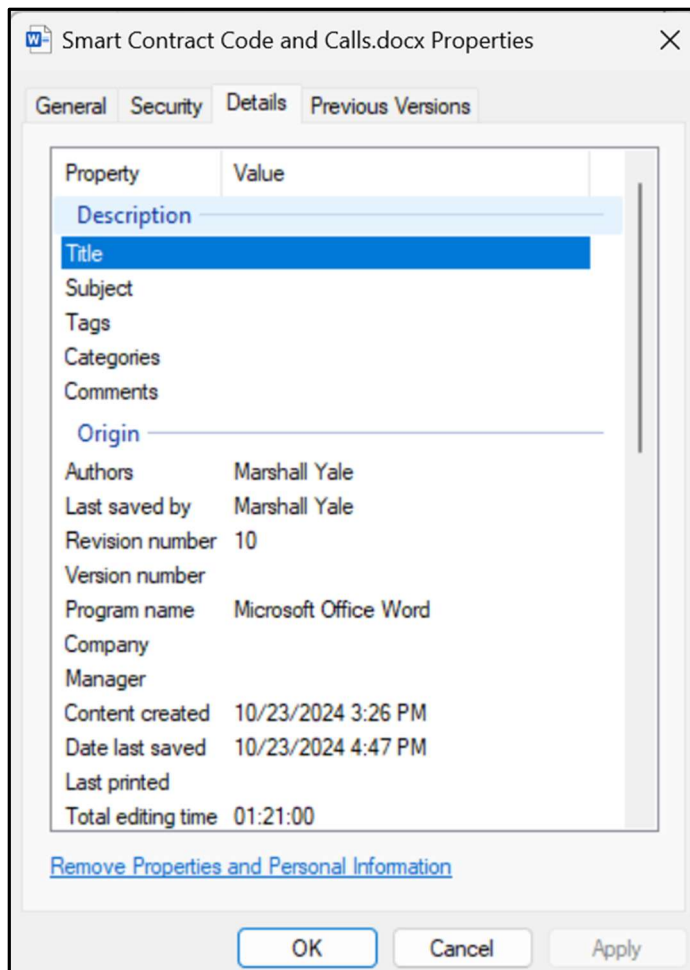
```

File Content Properties Hex Interpreter

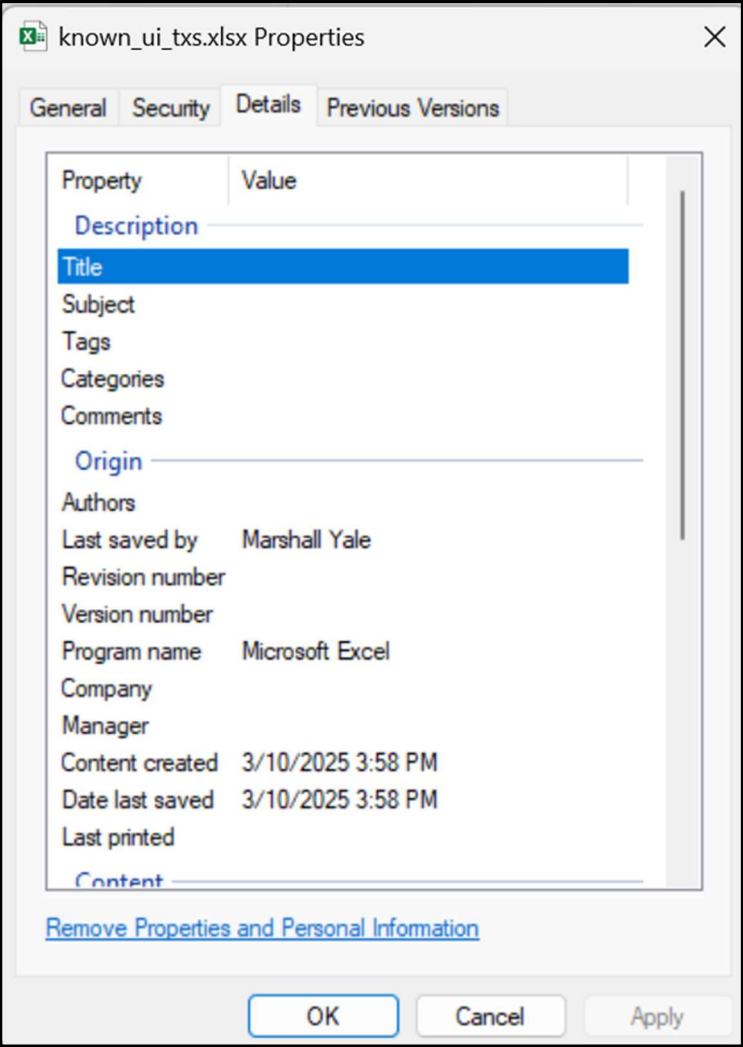
“dns_report_tc.xlsx” schema metadata

EXHIBIT P

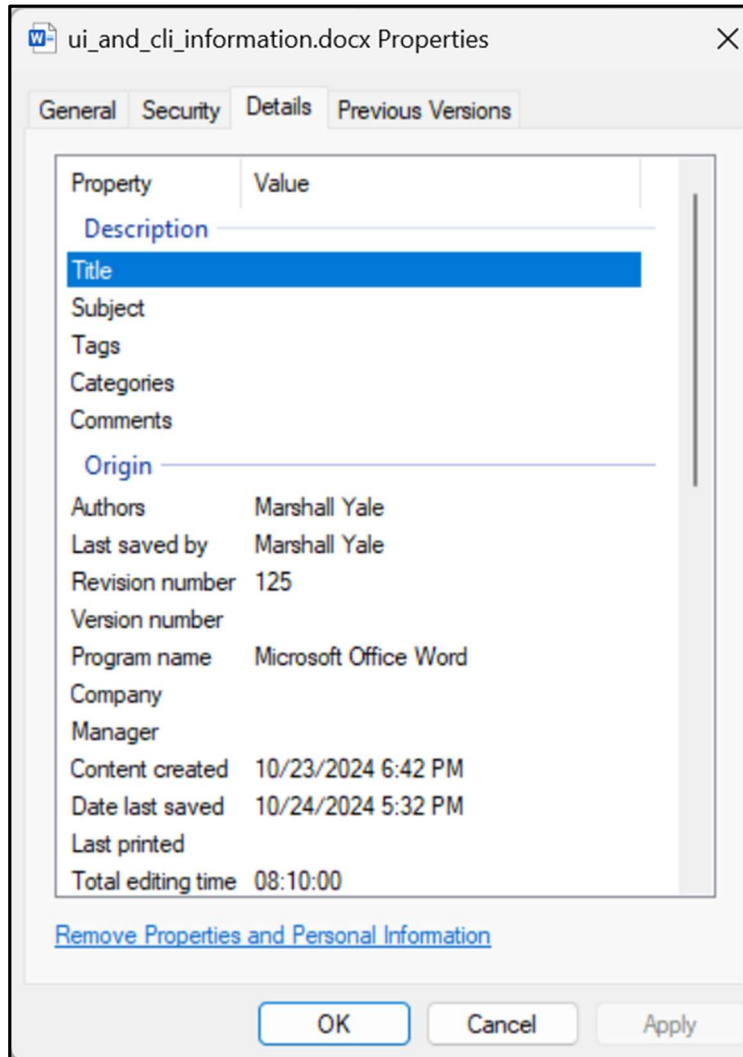
**MICROSOFT WINDOWS “FILE PROPERTIES”
FOR DOCUMENTS REVIEWED**



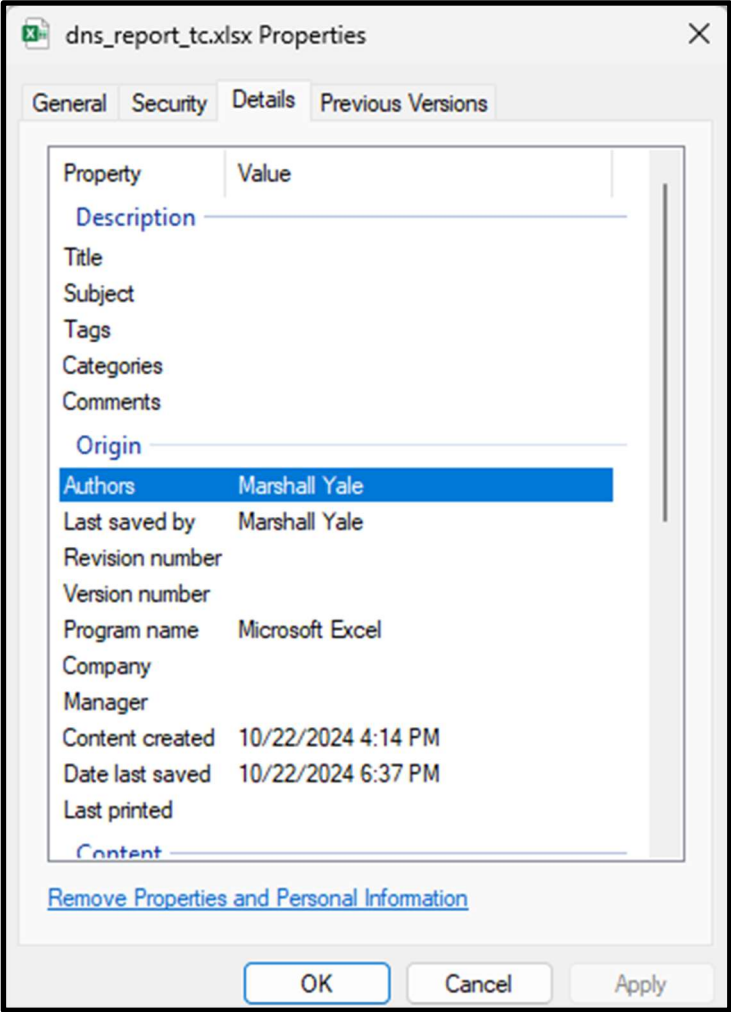
“Smart Contract Code and Calls.docx”



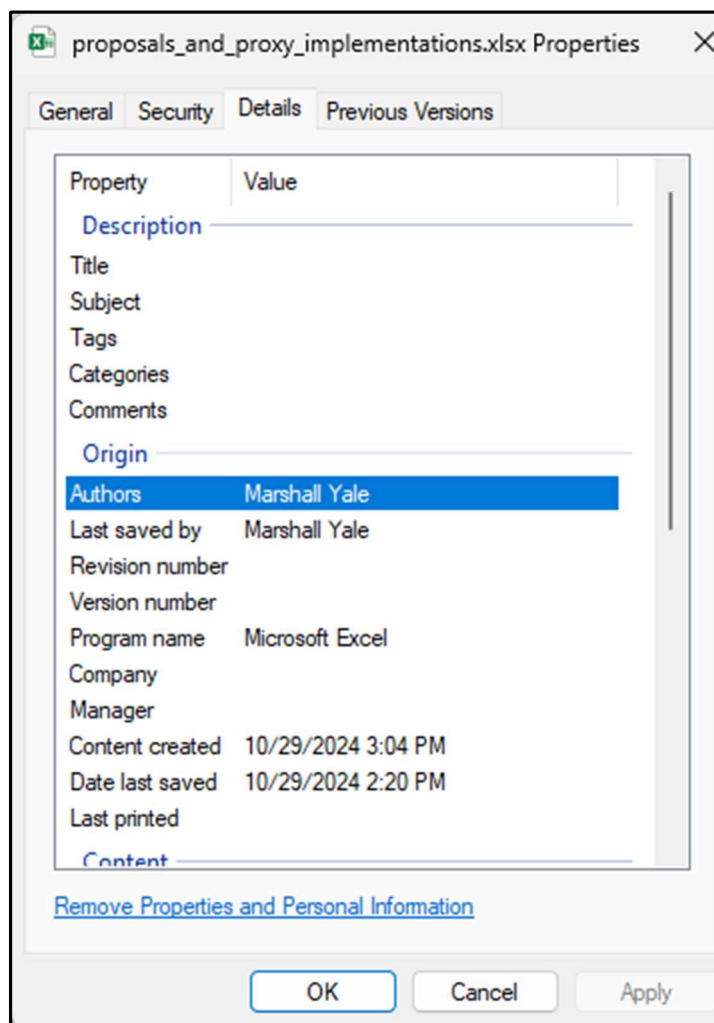
“known_ui_txs.xlsx”



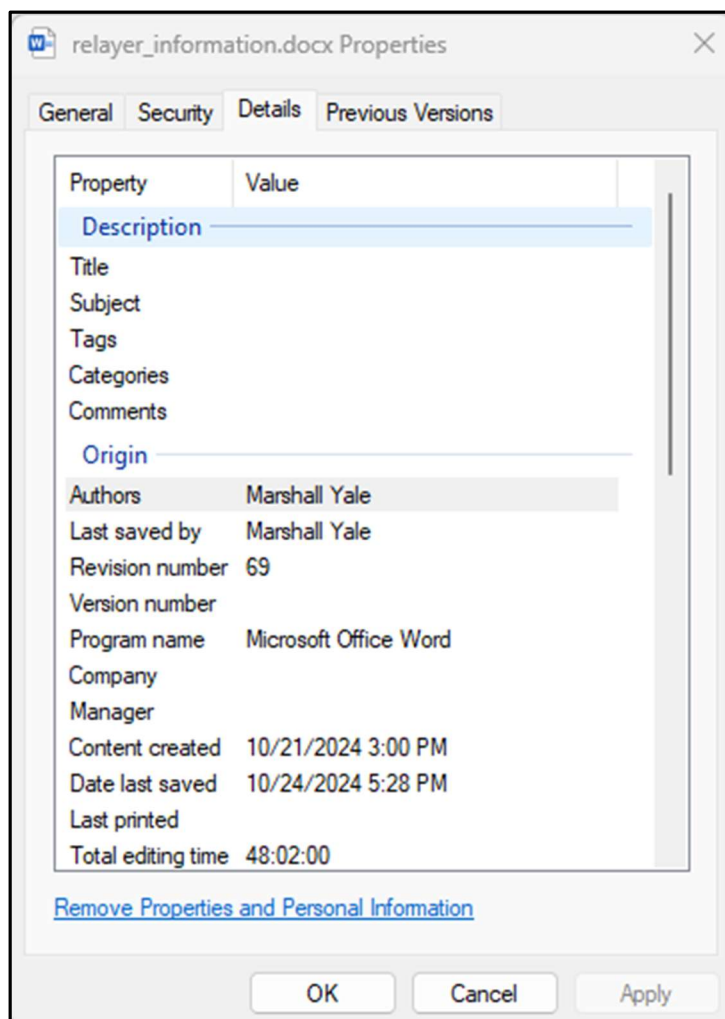
"ui_and_cli_information.docx"



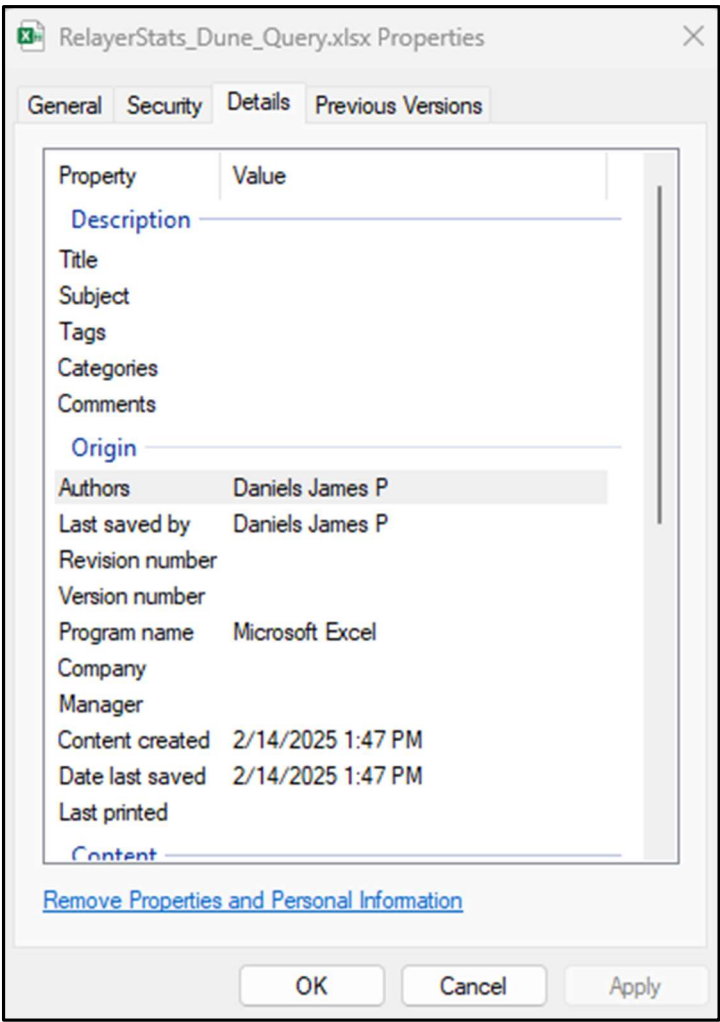
“dns_report_tc.xlsx”



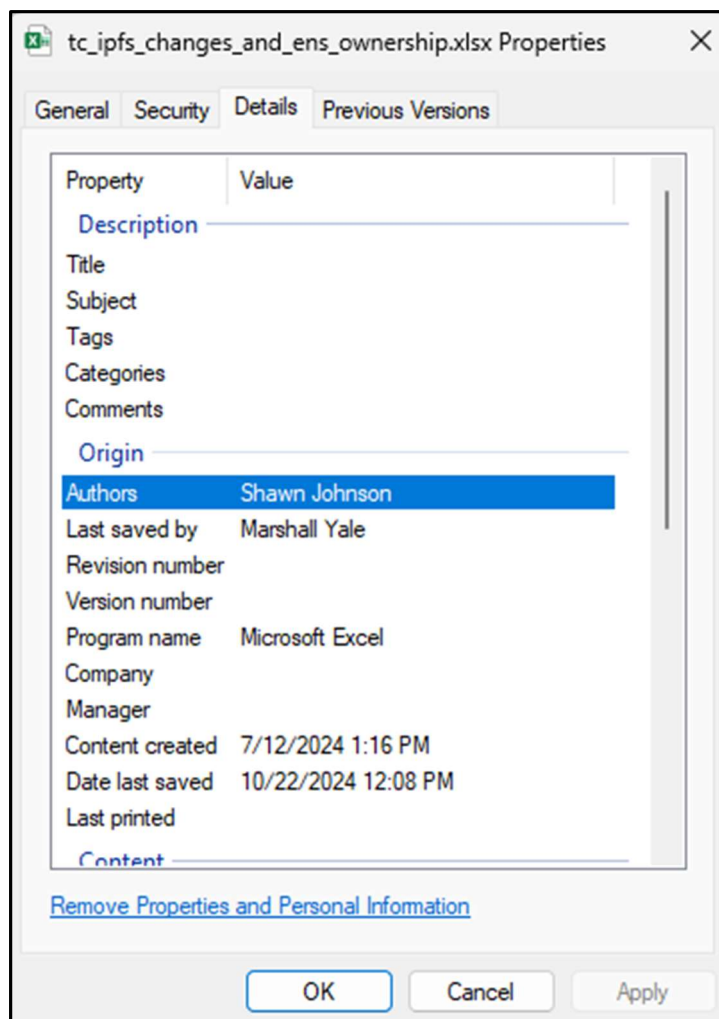
“proposals_and_proxy_implementations.xlsx”



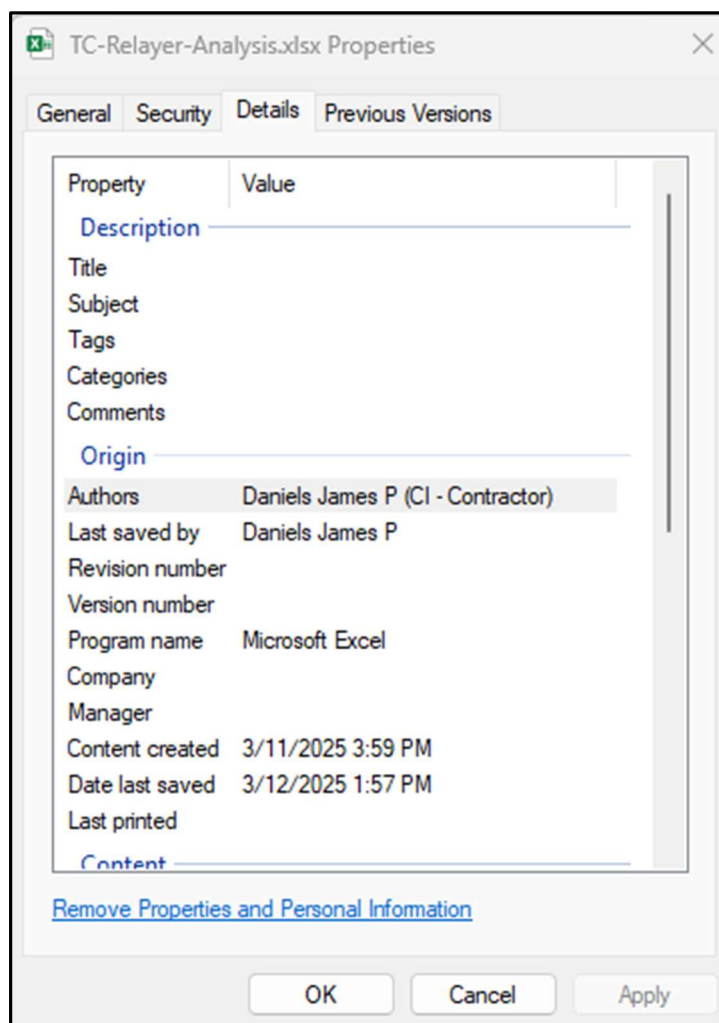
“relayer_information.docx”



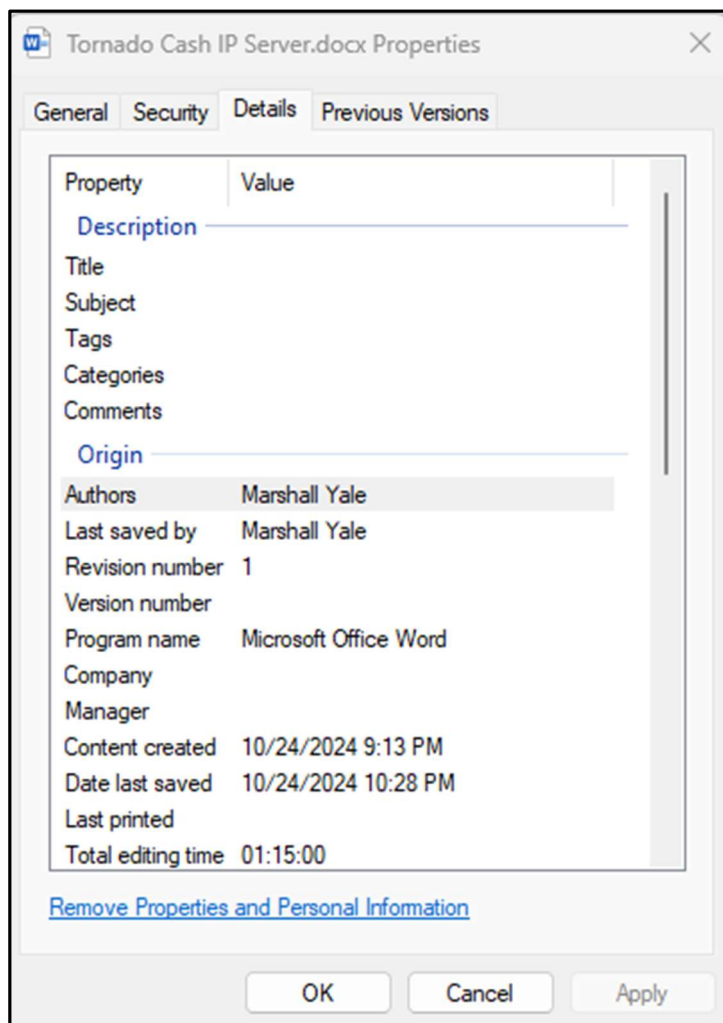
“RelayerStats_Dune_Query.xlsx”



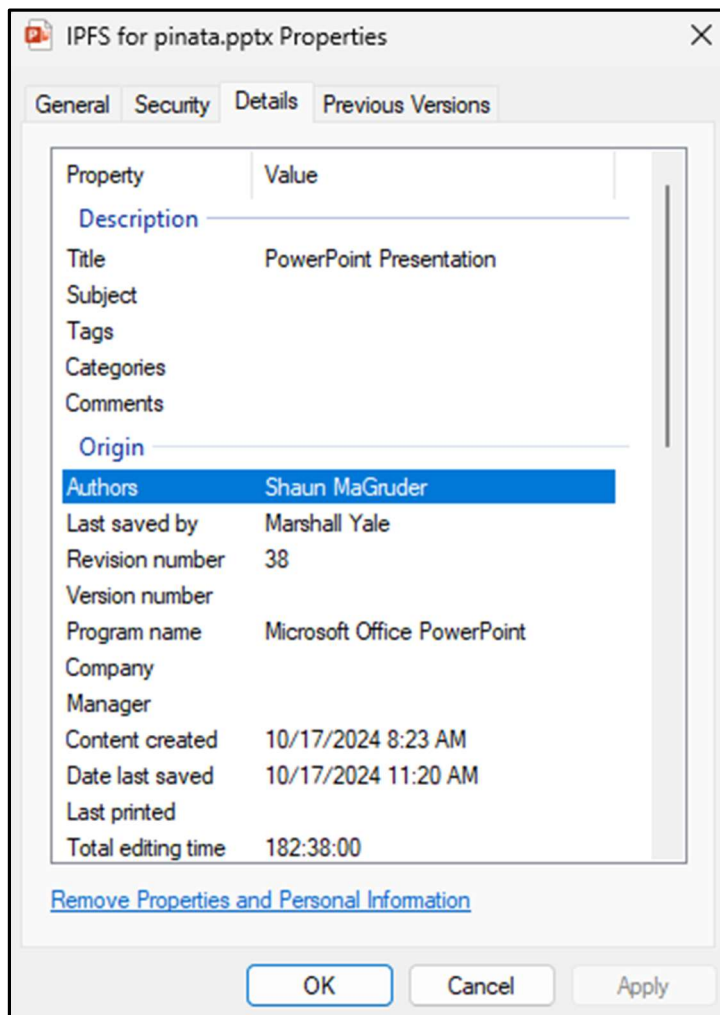
“tc_ipfs_changes_and_ens_ownership.xlsx”



"TC-Relayer-Analysis.xlsx"



“Tornado Cash IP Server.docx”



"IPFS for pinata.pptx"

EXHIBIT Q

**ADOBE ACROBAT READER
“DOCUMENT PROPERTIES”**

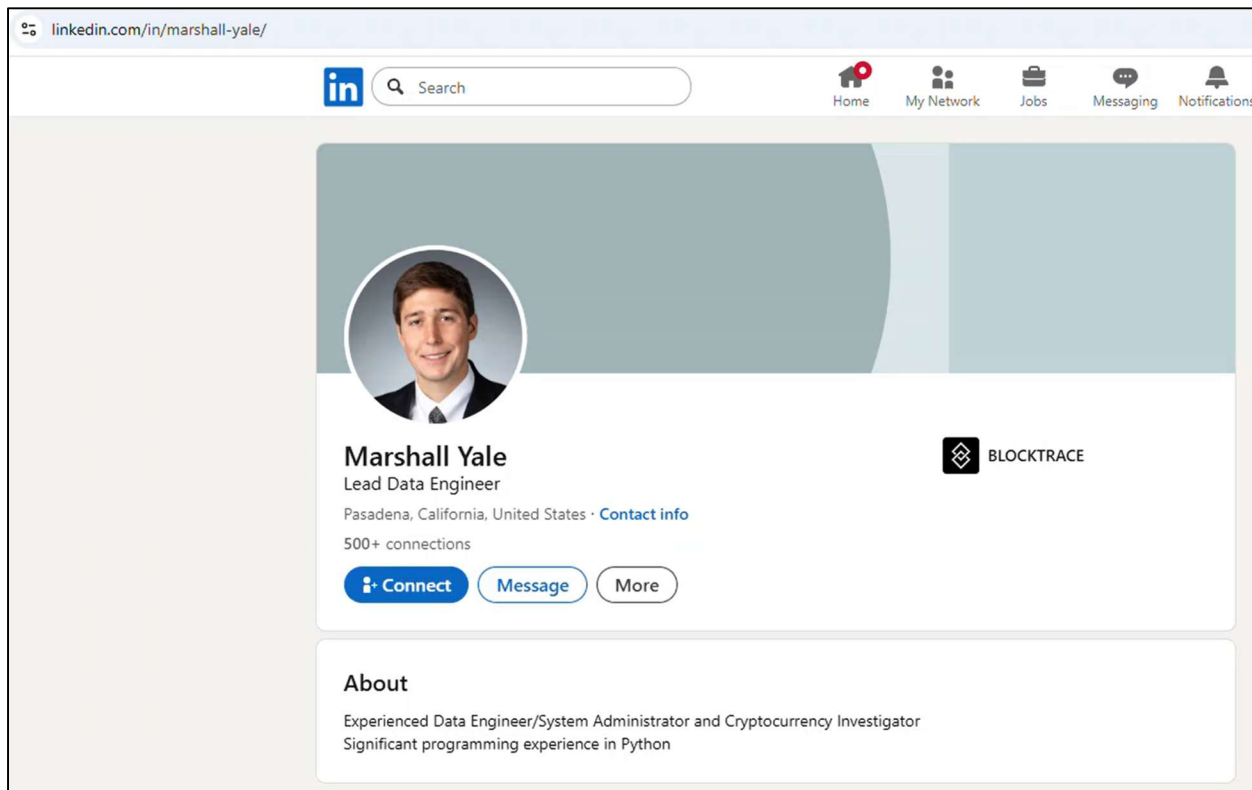
The screenshot shows the 'Document Properties' dialog box in Adobe Acrobat Reader. The 'Description' tab is selected, showing the following information:

- File:** Gas Analysis Methodology.pdf
- Title:** (empty text field)
- Author:** Marshall Yale
- Subject:** (empty text field)
- Keywords:** (empty text area)
- Created:** 3/12/2025 11:02:33 PM
- Modified:** 3/12/2025 11:02:37 PM
- Application:** Acrobat PDFMaker 24 for Word


“Gas Analysis Methodology.pdf”

EXHIBIT R


MARSHALL YALE LINKEDIN PROFILE SCREENSHOTS




linkedin.com/in/marshall-yale/


 Search

Home My Network Jobs Messaging Notifications


 **Marshall Yale**
Lead Data Engineer


Experience


Lead Data Engineer
 BLOCKTRACE · Full-time
 Oct 2021 - Present · 3 yrs 9 mos
 Python (Programming Language), Cryptocurrency and +1 skill


Lockheed Martin
 2 yrs 8 mos

- Data Engineer**
 Jun 2020 - Oct 2021 · 1 yr 5 mos
 Managed a Neo4J graph database project using Cypher, SQL, and Python which interfaces with different RDBMSs including SAP Hana, SQL Server, and Oracle... [...see more](#)
- Associate Space Systems Engineer**
 Mar 2019 - Jun 2020 · 1 yr 4 mos
 Coordinated a successful \$500,000 System Requirements Review for a new program
 Led weekly meetings with 30+ attendees to accomplish a successful System Requirements Review... [...see more](#)


Propulsion Operations Intern, Ground Support Engineering
 Virgin Galactic
 Jun 2018 - Aug 2018 · 3 mos
 Mojave, CA
 Worked with Propulsion team in support of Spaceship 2
 Constructed electrical and plumbing schematics in support of propulsion ground support equipment. [...see more](#)


CFD, Aeromechanics Intern
 NASA Ames Research Center
 Aug 2017 - Dec 2017 · 5 mos
 Moffett Field